(12) UK Patent Application (19) GB (11) 2 332 833 (13) A

(43) Date of A Publication 30.06.1999

(21) Application No 9727369.2

(22) Date of Filing 24.12.1997

(71) Applicant(s)
Interactive Magazines Limited
(Incorporated in the United Kingdom)
Bodrennick, Flushing, FALMOUTH, Cornwall,
TR11 5TP, United Kingdom

(72) Inventor(s)
Simon Hichens

(74) Agent and/or Address for Service
J A Kemp & Co.
14 South Square, Gray's Inn, LONDON, WC1R 5LX,
United Kingdom

(51) INT CL[6]
G07F 7/10 , H04L 9/32 29/06

(52) UK CL (Edition Q)
H4P PDCSX PPEB
U1S S2124 S2271

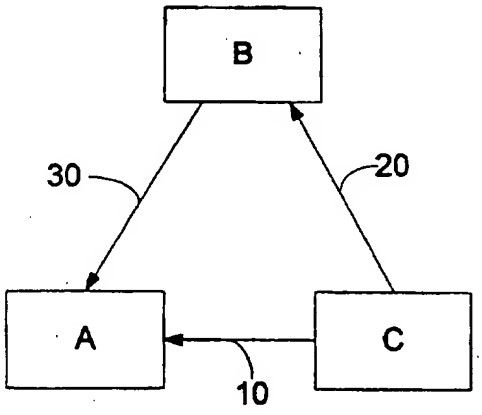
(56) Documents Cited
EP 0791901 A2 WO 96/36025 A2 WO 96/29667 A1
US 5590197 A US 4802220 A
COMPUTER Abstract Accession No. 02112564 &
Windows Sources Vol. 4, No. 11, November 1997,
p193

(58) Field of Search
UK CL (Edition P) H4P PDCSA PDCSC PDCSP PDCSS
PDCSX PPEB
INT CL[6] G07F 7/10 , H04L 9/00 9/14 9/28 9/30 9/32
12/22 29/06
Online:- WPI, INSPEC, JAPIO, IAC COMPUTER

(54) Abstract Title
Secure credit card transactions over the internet

(57) A first party C wishing to make a purchase over the Internet splits a message containing confidential information such as credit card number, name etc into two parts. A first part is sent to the seller or second party B, and the other part is sent directly to a trusted third party A such as a credit card company. The seller processes its part of the information and forwards it on to the trusted third party who is then in possession of all the information necessary to process the transaction. Even if one part of the message is intercepted, the security of the whole message is not necessarily compromised. The individual parts of the message may be encrypted and may incorporate public/private key systems. For certain transactions, a password or PIN number may be sent off line to the third party.

Fig. 1



par l'intermédiaire
≈ WO 96/29667

GB 2 332 833 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig. 1

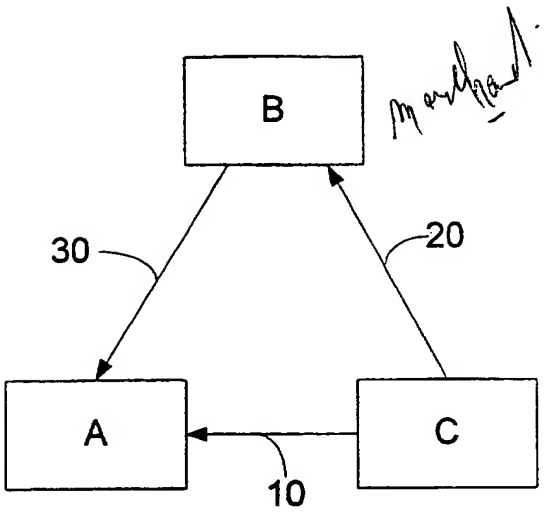
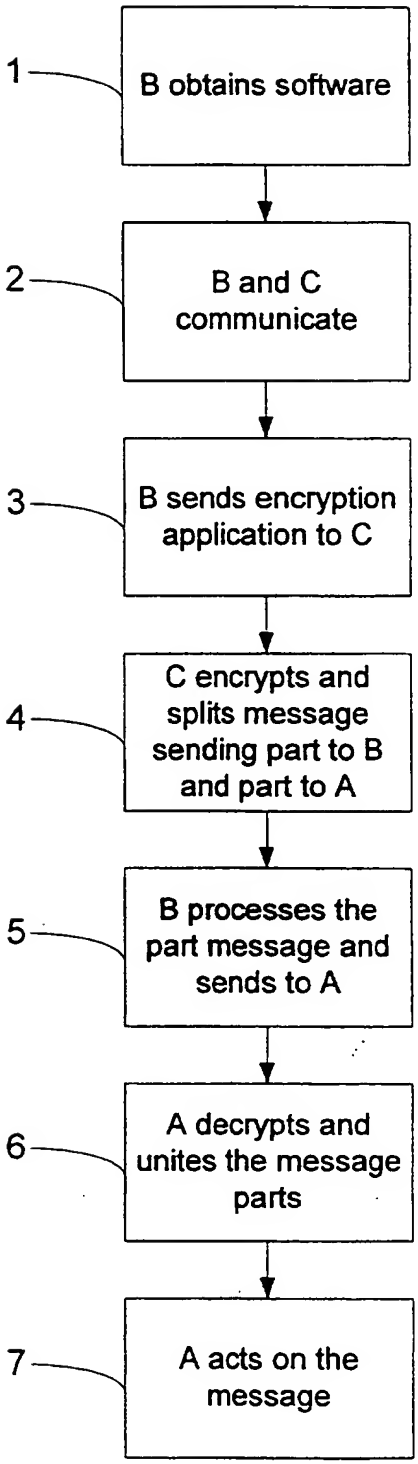


Fig. 2


1
B obtains software
2
B and C communicate
3
B sends encryption application to C
4
C encrypts and splits message sending part to B and part to A
5
B processes the part message and sends to A
6
A decrypts and unites the message parts
7
A acts on the message

2332833

MESSAGE COMMUNICATION METHOD

This invention relates to a method of communicating a message and in particular to improvements in security such as in an electronic network.

One data transfer method currently used on the Internet is known as PGP (pretty good privacy) public key/private key method. For transmitting data between a sender and a receiver, the receiver first randomly generates a public enciphering key and a secret deciphering key. The enciphering key and transformation algorithm or software can be publicly disseminated. The transformation uses operations that are easily performed, but difficult to invert. When the sender wishes to transmit a message to the receiver, the message is encrypted using the public key and transformation before it is transmitted. The receiver can use his secret deciphering key to recover the original message. Such a system is disclosed in US 4,218,582.

Although perceived as relatively safe, this method has the drawback that if the enciphered message is intercepted, powerful computers can now in fact decipher it without first knowing the receiver's private key. The messages are even more vulnerable if the algorithms are restricted to short keys such as forty bits. Further problems are the limited availability and lack of public acceptance of this method.

It is an object of this invention to alleviate, at least partially, some or all of the above problems.

Accordingly the present invention provides a method of communicating a message from a first party comprising the steps of:

splitting into first and second parts the message to be communicated by the first party;

sending the first part of the split message from the first party to a second party;

sending the second part of the split message from the first party to a third party;

processing at the second party the data which comprises the first part of the message and sending that part of the

message on to the third party;

receiving both parts of the message at the third party and uniting them to obtain the full message.

Splitting the data into two parts has the advantage that even if one part is intercepted the security of the whole message is not necessarily compromised. Sending the parts via different routes increases the security. The use of three parties encourages confidence in the method of communication since it is possible for each party to know at least one of the other parties in advance. The method also has the advantage that it enables a transaction to be performed with one of the parties never receiving the full transmitted data and permits a trusted third party to be involved for independent control and security.

Further optionally preferred features of the invention are included in the dependent claims. Advantages include increased security and the ability of a sender to transmit a secure message without itself previously holding a sophisticated encryption program.

Embodiments of the invention will now be described by way of example only, with reference to the accompanying drawings in which:

Fig. 1 shows an example of a communication involving three parties according to the invention; and

Fig. 2 shows stages of a method according to the invention.

Referring to Fig. 1, in a typical situation, a party C wants to perform a transaction with a party B which involves C sending sensitive information. For example, C might be a customer and B might be offering goods or services for sale via the Internet. C wants to make a payment to B, however it is not desirable for C to send e.g. a credit card number to B for two reasons. Firstly, an electronic message containing the credit card number might be intercepted by third parties and is not secure even if encrypted, which might result in

misuse of the credit card number, and secondly, C may not have established a relationship with B and might fear misuse of or insufficient security over its credit card number by B. In addition, both parties might be wary of a transaction with an unknown party purely via e-mail with no authentification of the other party.

Consequently, the following method is used, which is an example according to the invention, and will be described as a sequence of stages which are summarised in Fig. 2.

Stage 1.

B obtains software which will be used to implement the method. The software includes encrypting algorithm <1>. Another party referred to as A, holds a reference that software with unique algorithm <1> is used by B. In the present example, party A might be a credit card company. B may obtain the software from a network site, e.g. an Internet; web or FTP site, or off-line e.g. by means of a CD ROM. The software may be distributed directly by A or by another party, provided B is registered at A as user of that software and algorithm.

Stage 2.

C enters into correspondence with B. This could be by C visiting a World Wide Web site or other information source displaying opportunities available from B, and C then contacts B with the intent of exploring these opportunities. The correspondence may be partially automated for example by the web site sending an application to C which might be in the form of a Java (trademark) applet. The Java applet, being platform independent, could command C's web browser to execute automatically a preformatted e-mail. C could enter information such as name, quantity of items it is interested in purchasing. The applet ensures that the e-mail is correctly addressed to B and addressed as emanating from C. This avoids errors and falsifications of the address given by C. As an alternative to C approaching B via a web site or similar, B may make direct contact with C.

Stage 3.

B activates the software received at stage 1 and processes the correspondence from C indicating C's interest. The software randomly generates an encrypting algorithm <2> which might for example be expressed as a code comprising a sequence of numbers which represents operations to be performed on data to be encrypted. B retains the code for algorithm <2> and also registers a reference to the transaction with C. The software then sends an application, such as a Java applet from B to C. The application includes means for encoding according to the algorithm <2> and also the reference for the transaction. The references may be encrypted but identifiable as coming from B. The transmission from B to C may represent an offer in contractual terms.

Stage 4.

The application sent from B to C now runs on C's computer and may display the terms of the offer. There may be more than one offer available and there may be a time constraint such as a period for acceptance of the offer after which the offer expires. To accept the offer, in one version party C enters information into the application such as his name and credit card number and then activates an acceptance "button" provided by the application. The application then encrypts the entered information using a randomly generated algorithm <3>. The code defining algorithm <3> is appended to the encrypted message and the whole is then re-encrypted and split according to algorithm <2>. One part of the split message is sent to A and one part is sent to B, as indicated by arrows 10 and 20 in Fig. 1. In a simple form of splitting, the application transmits an encrypted acceptance to B and credit card details excluding name to A.

Further security measures could be taken to avoid the encryption algorithms from being cracked and hence the message being deciphered by an unauthorised party. One possibility is that the application that does the encrypting

destroys itself after use or after the offer has expired, another is that the application has a built-in time delay each time it is used or significantly expands in file size on each use. A further enhancement is staggering the sending of data to A and B. For instance C might break off his dial-up connection to the internet having sent the part of the message to B and then establish a direct connection to A to send the other part of the message. Similarly, one part of the message could be sent via a different medium to the other.

Stage 5.

B receives the part of the message from C, appends the code for algorithm <2> and then re-encrypts the message using algorithm <1> and sends the results to A, as indicated by arrow 30 in Fig. 1. B may then await confirmation from A concerning the credit card transaction before supplying the goods or services to C. For security, B could also destroy the message from C and the reference to algorithm <2>.

Stage 6.

A receives the messages from B and C which include reference to each other, e.g. by the transaction reference number B has already registered with A as user of algorithm <1>, so A can decrypt the highest level of encryption of the message from B which will reveal the appended code for algorithm <2>. A can then decrypt the algorithm <2> coding of the resulting message from B and the message from C. The reverse of algorithm <2> also unites the two parts of the split message and yields the appended decrypted code for algorithm <3>. The united message can finally be decrypted by the reverse of algorithm <3>. A should have a high level of so-called "fire wall" security to protect the decrypted information and other sensitive data in its records.

Stage 7.

A acts on the instructions in the deciphered message for example by debiting C's credit card account and/or crediting B's account. A might be an intermediary who instructs a

financial institution over a secure means regarding the transfer of funds in relation to the transaction between B and C.

Some further variations and optional features of the invention will now be described.

C might send B part of the message (e.g. name) at an earlier time in the correspondence such as at stage 2 rather than stage 4. B sends this onto A, preferably with encryption. C and A then communicate to complete the transaction.

Responsibility over security could be transferred to a fourth party, for example B sends its part of the encrypted message to the fourth party instead of to A. A also forwards its part of the message from C to the fourth party. The fourth party then decrypts and unites the message.

The operations performed by B may be automated to some extent. For example the software associated with algorithm <1> could do one or more of the following:

recognise interest from C and send out the appropriate offer application and algorithm <2>;

securely reference the transaction to algorithm <2>;

recognise returned acceptances, process them and update appropriate records;

send out encrypted messages to A; and

destroy the message received from C and references to algorithm <2>.

For certain transactions, a password or personal identification number (PIN) may be used. A could send C a password or PIN off line by any safe medium other than that used for the transaction. For example, C could receive a PIN by post from a bank A. C would then include the PIN in the message that is encrypted and transmitted to A. On decryption, A would verify the PIN before effecting the transaction. The PIN can be changed off-line as often as required.

Some simple illustrative examples of the encrypting

algorithms are as follows:

firstly the information entered by C, such as credit card number and name, is converted into a sequence of numbers, for example using those corresponding to a standard character set e.g. ASCII. Algorithm <3>, which is randomly generated by the application at C, is then applied to the sequence of numbers. An example might be: to each number add 9 and the previous result. (In these examples all arithmetic is done in modulo 256 or whatever the total number of character codes being used is). The operations of algorithm <3> can be represented compactly as a short sequence of digits which can be interpreted by deciphering software to reverse the algorithm. The short sequence of digits is referred to as the algorithm code.

Algorithm <2> is randomly generated at B in the embodiment described above, and is also representable by a code series of numbers, which are registered at B. Algorithm <2> can include both encrypting and splitting operations, for example:

Step 1:

Take the message encrypted according to algorithm <3>; place the algorithm <3> code at the beginning; add 1 to the 1st number, 3 to the 2nd number and 7 to the 3rd and repeat for the 4th, 5th and 6th numbers and so on.

Step 2:

Split the resulting sequence of numbers by placing the 1st, 3rd, 5th and odd position numbers in message 1 and the numbers in the even positions in message 2; reverse the order of the numbers in messages 1 and 2; add a reference number to the transaction to the end of each message.

Message 1 is then sent to B and message 2 to A. B then performs algorithm <1> on message 1. Examples of the operations of algorithm <1> are: place the code for algorithm <2> in reverse order starting from position 6 in message 1 received from C. Add 12 to the first number 25 to the second number and repeat for every pair of numbers, place numbers

representing the amount of money to be transferred at the end and include a code number indicating currency; add 26 to all values plus 6 for each place from the beginning; include a reference to the transaction and party B; finally send to A (A already knows algorithm <1>, for example by its algorithm code, and that B is registered as user of that algorithm).

Much more complex algorithms can of course be used for example including a public key/private key system.

CLAIMS

1. A method of communicating a message from a first party comprising the steps of:

splitting into first and second parts the message to be communicated by the first party;

sending the first part of the split message from the first party to a second party;

sending the second part of the split message from the first party to a third party;

processing at the second party the data which comprises the first part of the message and sending that part of the message on to the third party;

receiving both parts of the message at the third party and uniting them to obtain the full message.

2. A method according to claim 1, further comprising the steps of:

applying at the first party a first encryption device so that one or both parts of the split message are encrypted before being sent;

sending a reference to the first encryption device to said third party; and

applying the reverse of the first encryption device at the third party to produce a decrypted united message.

3. A method according to claim 1 or 2, wherein the step of processing comprises:

applying at the second party a second encryption algorithm to said first part of the split message before sending that part on to the third party; and

sending reference to the second encryption device to the third party,

and wherein the method further comprises the step of applying the reverse of the second encryption device to said first part of the message received at the third party.

4. A method according to claim 2 or claim 3 when appendent to claim 2, further comprising the steps of:

randomly generating the first encryption device at the second party; and

sending the first encryption device from the second party to the first party.

5. A method according to claim 4, further comprising the step of:

sending an offer with said first encrypting device, from said second party to said first party, wherein said first party has a limited period of time in which to respond to the offer.

6. A method according to claim 4 or 5, further comprising the step of:

sending from the second party to the first party an application which includes the randomly generated first encryption device and also includes a device for splitting and sending the data.

7. A method according to claim 6, wherein said application is in the form of a non-platform specific computer program.

8. A method according to claim 6 or 7, further comprising the steps of:

generating a random third encryption device by the application at the second party; and

applying said third device to the message to be communicated before the message is encrypted by said first encryption device, split and sent.

9. A method according to any one of the claims 3 to 8, wherein said second encryption device forms part of an application which controls the sending, encrypting and splitting of messages, and wherein said second encryption

device is referenced to the second party in records available to the third party.

10. A method according to any one of the preceding claims, wherein there is a time delay between sending the first and second parts of the message from the first party.

11. A method according to any one of the preceding claims, wherein said first party uses a password to authenticate transmissions, said password being known by said third party and being communicated to said first party by means other than those used for sending said message.

12. A method according to any one of the preceding claims, wherein said message is sent over an internet, extranet or intranet.

Patent Office

12

Application No: GB 9727369.2
Claims searched: 1-12

Examiner: Matthew Nelson
Date of search: 13 May 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PDCSA, PDCSC, PDCSP, PDCSS, PDCSX, PPEB)

Int Cl (Ed.6): H04L 9/00, 9/14, 9/28, 9/30, 9/32, 12/22, 29/06; G07F 7/10

Other: Online:- WPI, JAPIO, INSPEC, COMPUTER

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	EP 0791901 A2 (CARD CALL) See whole document	
A	WO 96/36025 A2 (NAT. WEST) See figure 1 & p. 8, line 17 - p. 9	
X	WO 96/29667 A1 (SANDBERG-DIMENT) See whole document	1, 2-4, 10 & 12 at least
A	US 5590197 (CHEN & WANG) See whole document	
A	US 4802220 (MARKER) See col. 1, line 58 - col. 2, line 22	
A	COMPUTER Abstract Accession No. 02112564 & Window Sources, Vol. 4, No. 11, November 1997, R Young "Transactions", page 193 (see abstract)	

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family

A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.